

IN THE CLAIMS:

Please ADD claim 22 as follows.

1. (Previously Presented) Authentication method for a telecommunications network, the method including the steps of

generating a set of subscriber-specific authentication data blocks into the network, each data block containing a challenge, a response and a key, whereby the generation is performed in the same manner as in ~~the~~ a known mobile communications system,

transmitting at least some of the challenges contained in the authentication data blocks to the terminal,

choosing one of the challenges for use in the terminal, and based on the challenge, determining a response and a key to be used with an aid of an identification unit of the terminal essentially in the same way as in a subscriber identification module of the mobile communication system,

determining an authenticator with an aid of the chosen key in the terminal,

transmitting from the terminal to the network authenticator and a data unit, the data unit containing information relating to the manner in which the authentication is formed and notifying the network with the aid of the data unit of which key corresponding to which challenge was chosen, and

a check value with the aid of the chosen key in the network, and

comparing the check value with the authenticator.

2. (Previously Presented) Method as defined in claim 1, wherein the data unit is a SPI (Security Parameter Index) in the registration message of the mobile IP protocol.

3. (Previously Presented) Method as defined in claim 1, wherein the value of the response determined at the terminal is inserted into the data unit.

4. (Previously Presented) Method as defined in claim 1, wherein the challenges are sorted in an order at the terminal with the aid of predetermined sorting criteria and a consecutive number corresponding to the chosen challenge is inserted into the data unit.

5. (Previously Presented) Method as defined in claim 1, wherein the identification unit used in the terminal is the subscriber identity module used by the known GSM system and the authentication data blocks are authentication triplets used by the GSM system.

6. (Previously Presented) Method as defined in claim 5, wherein the authentication triplets are fetched from the authentication centre of the GSM system.

7. (Previously Presented) Method as defined in claim 6, wherein the challenges to be transmitted to the terminal are transmitted by using a known short message switching service.

8. (Previously Presented) Method as defined in claim 1, wherein the challenges to be transmitted to the terminal are transmitted in an IP datagram to be sent through an IP network.

9. (Previously Presented) Method as defined in claim 1 for an IP network, wherein the authentication data blocks are transmitted to the home agent of the terminal and with the aid of the data unit message is given to the home agent about which key corresponding to which challenge was chosen, whereby the check value is determined in the home agent.

10. (Previously Presented) Authentication system for a telecommunications network, the system including

in a terminal of the network, first message transmission means for transmitting an authenticator and a data unit to the network, the data unit including information relating to the manner in which the authenticator is formed, and

checking means for determining a check value with aid of the data unit,

wherein

the terminal of the network includes such an identification unit, which receives as input a challenge from which a response and a key are defined essentially in a same manner as in a subscriber identity module of a known mobile communications system,

the system includes generating means for generating authentication data blocks in the same manner as in the mobile communications system, the authentication data blocks include a challenge, a response and a key,

the system includes transmission means for transmitting challenges contained by the authentication data blocks to the terminal, and

the terminal includes selection means for selecting one challenge for use,

the first message transmission means insert such a value into the data unit which indicates which key corresponding to which challenge was selected for use in the terminal, and

the first message transmission means determine the authenticator and the checking means determine the check value based on the selected key.

11. (Previously Presented) System as defined in claim 10, wherein the identification unit located in connection with the terminal is a subscriber identity module used in the mobile communications system.

12. (Previously Presented) System as defined in claim 10, wherein the said generating means include an authentication centre of the mobile communications

system.

13. (Previously Presented) System as defined in claim 10, wherein the said transmission means include means for carrying out a known short message switching service.

14. (Previously Presented) An authentication method for a telecommunications network, said method comprising:

generating a set of subscriber-specific authentication data blocks, each authentication data block containing a challenge, a response and a key,

transmitting at least some of the challenges contained in the authentication data blocks to a terminal,

receiving an authenticator and a data unit containing information relating to a manner in which the authenticator is formed from the terminal,

determining based on said data unit which challenge was chosen by the terminal, and

determining a check value with the key corresponding to the chosen challenge, said check value to be compared with the authenticator.

15. (Previously Presented) An authentication method as defined in claim 14, wherein said data unit is a security parameter index in the registration message of a Mobile IP protocol.

16. (Previously Presented) An authentication method as defined in claim 14, wherein said data unit comprises the response corresponding to the chosen challenge.

17. (Previously Presented) An authentication method for a terminal, said method comprising:

receiving a set of challenges from a telecommunications network,
choosing one challenge from the set of challenges,
determining a response and a key based on the chosen challenge,
determining an authenticator based on the key corresponding to the chosen challenge, and
transmitting said authenticator and a data unit to the telecommunications network, said data unit relating to the manner in which the authenticator is formed and notifying the telecommunications network of the chosen challenge.

18. (Previously Presented) An authentication method as defined in claim 17, wherein said data unit is a security parameter index in the registration message of a Mobile IP protocol.

19. (Previously Presented) An authentication method as defined in claim 17, wherein said data unit comprises the response corresponding to the chosen challenge.

20. (Previously Presented) A telecommunications network configured to generate a set of subscriber-specific authentication data blocks, each authentication data block containing a challenge, a response and a key, transmit at least some of the challenges contained in the authentication data blocks to a terminal, receive an authenticator and a data unit containing information relating to a manner in which the authenticator is formed, determine based on said data unit which challenge was chosen by the terminal, determine a check value with the key corresponding to the chosen challenge, said check value to be compared with the authenticator.

21. (Previously Presented) A terminal for a telecommunications network, said terminal configured to receive a set of challenges from a telecommunications network, choose one challenge from the set of challenges, determine a response and a key based on the chosen challenge,

determine an authenticator based on the key corresponding to the chosen challenge, and

transmit said authenticator and a data unit to the telecommunications network, said data unit relating to the manner in which the authenticator is formed and notifying the telecommunications network of the chosen challenge.

22. (New) An apparatus of a telecommunications network, the apparatus comprising:

generating means for generating a set of subscriber-specific authentication data blocks into the network, each data block containing a challenge, a response and a key, whereby the generation is performed in the same manner as in the a known mobile communications system;

transmitting means for transmitting at least some of the challenges contained in the authentication data blocks to the terminal;

choosing means for choosing one of the challenges for use in the terminal, and based on the challenge, determining a response and a key to be used with an aid of an identification unit of the terminal essentially in the same way as in a subscriber identification module of the mobile communication system;

determining means for determining an authenticator with an aid of the chosen key in the terminal;

transmitting means for transmitting from the terminal to the network authenticator and a data unit, the data unit containing information relating to the manner in which the authentication is formed and notifying the network with the aid of the data unit of which key corresponding to which challenge was chosen, and a check value with the aid of the chosen key in the network; and

comparing the check value with the authenticator.